Compute-and-Forward Can Buy Secrecy Cheap

Parisa Babaheidarian*, Somayeh Salimi**
*Boston University,**KTH Royal Institute of Technology

***Abstract*—We consider a Gaussian multiple access channel with K transmitters, a (intended) receiver and an external eavesdropper. The transmitters wish to reliably communicate with the receiver while concealing their messages from the eavesdropper. This scenario has been investigated in prior works using two different coding techniques; the random i.i.d. Gaussian coding and the signal alignment coding. Although, the latter offers promising results in a very high SNR regime, extending these results to the finite SNR regime is a challenging task. In this paper, we propose a new lattice alignment scheme based on the compute-and-forward framework which works at any finite SNR. We show that our achievable secure sum rate scales with $\log(\text{SNR})$ and hence, in most SNR regimes, our scheme outperforms the random coding scheme in which the secure sum rate does not grow with power. Furthermore, we show that our result matches the prior work in the infinite SNR regime. Additionally, we analyze our result numerically.**

I. Introduction

Gaussian Multiple Access Channel (MAC) has been considered under different security scenarios. One interesting scenario is the K-user Gaussian MAC with an external eavesdropper in which the users wish to reliably send their messages to the receiver while keeping them hidden from the eavesdropper. This scenario has been investigated in [1] using the Gaussian i.i.d. random codes. Although, these codes achieve the capacity region of MAC without security, the result in [1] shows that they have a poor performance in relatively high SNR regimes when the security constraint is added. In an attempt to improve the high SNR results, researchers investigated the problem using the signal alignment technique. In particular, in [2] and [3], it is shown that their proposed schemes offer a significant improvement over the random coding counterpart in a very high SNR regime. In fact, the scheme proposed in [3] achieves the optimal secure Degrees of Freedom (DoF) of the K-user Gaussian wiretap MAC. However, as these alignment schemes use a maximum-likelihood decoder, bounding the error probability of the decoder in the finite SNR regime is challenging and this limits their results to the high SNR regime.

In light of lattice alignment technique, the compute-and-forward framework was proposed in [4] which can operate at any finite SNR. Recently, the K-user Gaussian MAC without security constraint has been investigated in [5] based on lattice coding and the compute-and-forward framework. The proposed scheme in [5] achieves the MAC sum capacity within a constant gap and for any finite SNR.

Motivated by the above arguments, we propose a new achievability scheme for the K-user Gaussian wiretap MAC in which lattice alignment is used along with the asymmetric compute-and-forward framework. We evaluate the performance of our proposed scheme both analytically and numerically for any finite SNR. We prove that our proposed scheme achieves a secure sum rate that scales with $\log(\text{SNR})$, in contrast to the Gaussian random coding result which does not grow with SNR and therefore, it somehow fails at moderate and high SNR regimes. Finally, we show that the asymptotic behavior of our proposed scheme agrees with the prior work result in [2] in the high SNR regime.

The paper is organized as follows. In Section II, our setup preliminaries are described. Our main result is given in Section III along with the comparison to the prior works. In Section IV, the proof of the main result is presented. We conclude the paper in Section V. The proof of Lemma 1 used in Section IV is given in Appendix.

II. Problem Statement

A K-user (real) Gaussian wiretap multiple access channel (MAC) consists of K transmitters, a receiver and an external eavesdropper. The relations between the channel inputs and outputs are given as

$$\mathbf{y} = \sum_{\ell=1}^{K} h_\ell \mathbf{x}_\ell + \mathbf{z}, \quad \mathbf{y}_E = \sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell + \mathbf{z}_E \tag{1}$$

where $\mathbf{x}_\ell$ is an N-length channel input vector of user ℓ which satisfies the following power constraint.

$$\|\mathbf{x}_\ell\|^2 \leq NP, \quad \forall \ell \in \{1,\dots,K\} \tag{2}$$

The vectors $\mathbf{y}$ and $\mathbf{y}_E$ in (1) are the receiver and the eavesdropper channel outputs, respectively. Also, $\mathbf{z}$ and $\mathbf{z}_E$ are the independent channel noises, each distributed i.i.d. according to $\mathcal{N}(0,1)$. Finally, vectors $\mathbf{h} \triangleq [h_1,\dots,h_K]^T$ and $\mathbf{g} \triangleq [g_1,\dots,g_K]^T$ are real-valued vectors representing the channel gains to the receiver and the eavesdropper, respectively. The channel model is illustrated in Fig. 1.

User ℓ encodes its confidential message W_ℓ, which is uniformly distributed over the set $\{1,\dots,2^{NR_\ell}\}$ and is independent of other users' messages, through some stochastic mapping $\mathcal{E}_\ell$, i.e., $\mathbf{x}_\ell = \mathcal{E}_\ell(W_\ell)$, for $\ell \in \{1,\dots,K\}$. There is also a decoder D at the receiver side which estimates the messages, i.e., $D(\mathbf{y}) = \{\hat{W}_\ell\}_{\ell=1}^{K}$.

Definition 1 (Achievable secure sum rate): For the described channel model, a secure sum rate $\sum_{\ell=1}^{K} R_\ell$ is achievable, if for any $\epsilon > 0$ and large enough N, there exist a sequence of encoders $\{\mathcal{E}_\ell\}_{\ell=1}^{k}$ and a decoder D such that

$$\Pr\left(\bigcup_{\ell=1}^{K}\{\hat{W}_\ell \neq W_\ell\}\right) < \epsilon \tag{3}$$

$$\sum_{\ell=1}^{K} R_\ell \leq \frac{1}{N} H(W_1, W_2, \dots, W_K|\mathbf{y}_E) + \epsilon \tag{4}$$

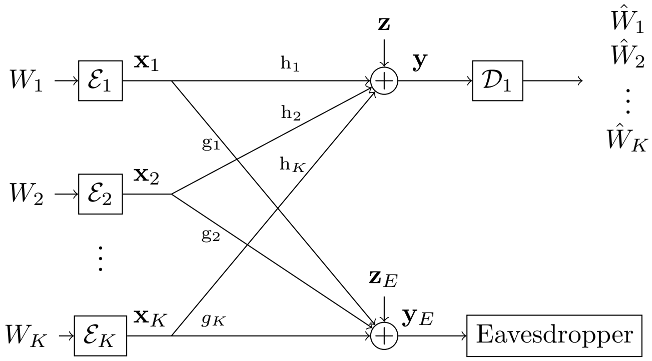

Fig. 1: The asymmetric Gaussian wiretap multiple access channel model.

where $\Pr$ denotes the probability of the event.[1] The secure sum capacity is the supremum of all achievable secure sum rates.

III. Main Results

The problem described in Section II has been treated in [2] and [3] in the infinite SNR regime. Their proposed schemes is based on bounding the minimum distance between the codewords in the receiver's effective codebook. Using this method, they showed that the decoding error probability tends to zero, provided that the input power goes to infinity. In this paper, we present a new scheme which provides a lower bound on the secure sum capacity for the same model and for any finite value of SNR. To this end, we utilize the compute-and-forward framework presented in [4]. More precisely, we develop a coding scheme using an asymmetric compute-and-forward framework to address the asymmetric transmitter-eavesdropper channel gains, i.e., different values of g_ℓ for different users. It should be noted that the asymmetric compute-and-forward framework is also treated in [6], but here we add the security constraint to the framework.

In the compute-and-forward framework, the receiver first decodes K linearly independent integer combinations of the transmitted lattice codewords and then, it solves the equations for its desired lattice codewords.[2] The equations are decoded successively meaning that at each step k, the receiver cancels the effect of the $k-1$ previously decoded codewords from the current equation and solves it for the next codeword. The approach is similar to the Gaussian elimination with a difference that row switching is not allowed here. This limitation is due to the fact that a codeword cannot be eliminated from the current equation using another equation which has not been decoded yet. As a result, the order of canceling out the codewords cannot be chosen arbitrarily, however, it can be shown that there exists at least one successive cancellation order such that all K codewords can be decoded [5].

Proposition 1: Consider an index permutation function π, i.e., $\pi : \{1, \ldots, K\} \rightarrow \{1, \ldots, K\}$, which gives a successive cancellation order in the compute-and-forward framework. Also, assume that the set of linearly independent integer-valued K-length vectors $\{\mathbf{a}_1, \ldots, \mathbf{a}_K\}$ be the equations coefficients. Then, for the channel model in Section II, the receiver can decode the message $W_\ell \in \{1, \ldots, 2^{NR_\ell}\}$ with a vanishing error probability if

$$R_\ell \leq R_{comb,\pi(\ell)} \triangleq \max\left(\frac{1}{2}\log\left(\frac{\mathrm{SNR}_\ell}{\|\mathbf{F}\ \mathbf{a}_{\pi(\ell)}\|^2}\right), 0\right) \qquad (5)$$

where the matrix $\mathbf{F}$ is given as

$$\mathbf{F} \triangleq \left(\frac{1}{P}\mathbf{I}_{K\times K} + \mathbf{h}\mathbf{h}^T\right)^{\frac{-1}{2}} \times \mathrm{diag}\left(\sqrt{\frac{\mathrm{SNR}_1}{P}}, \ldots, \sqrt{\frac{\mathrm{SNR}_K}{P}}\right).$$

The notation $\mathrm{diag}(\mathbf{v})$ stands for the diagonal matrix built from the vector $\mathbf{v}$ and $\mathrm{SNR}_\ell > 0$ is the power used at encoder ℓ to generate its codewords. Notice that as long as the generated codewords are scaled properly before transmission, they would satisfy the channel input power constraint.[3]
Proposition 1 is immediately deduced from applying Theorem 2 along with Theorem 5 in [5] with an exception that, here, users operate at different powers. All other conditions stated in Theorem 5 in [5] still apply in Proposition 1.

In the following, we present a lower bound on the secure sum capacity achieved by the proposed scheme.

Theorem 1: A rate tuple $(R_1, \ldots, R_K)$ offers an achievable secure sum rate for the channel model described in Section II, if they satisfy the following constraints.

$$R_\ell \geq 0,\ R_\ell \leq R_{comb,\pi(\ell)} \quad \forall \ell \in \{1, \ldots, K\} \qquad (6)$$

$$\sum_{\ell=1}^{K} R_\ell \leq \max_{\pi} R_{\textbf{sum}} \qquad (7)$$

where

$$R_{\textbf{sum}} = \left(\sum_{k=2}^{K} R_{comb,k} - \frac{1}{2}\log\left(\frac{\sum_{\ell=1}^{K} g_\ell^2}{g_{\pi^{-1}(1)}^2}\right)\right) \qquad (8)$$

The maximum in (7) is taken over all the possible successive cancellation orders π and the notation $\pi^{-1}(.)$ simply denotes the inverse permutation operator.
Proof of Theorem 1 is given in Section IV.

Comparison to the prior works

The K-user Gaussian wiretap MAC has been investigated in [1] by means of i.i.d. Gaussian random coding. According to [1], for the considered channel model, the following secure sum rate is achievable

$$\sum_{\ell=1}^{K} R_\ell \leq \max\left(\frac{1}{2}\log\left(\frac{1 + \|\mathbf{h}\|^2 P}{1 + \|\mathbf{g}\|^2 P}\right), 0\right) \qquad (9)$$

Note that the right hand side of expression (9) does not scale with power P or in other words, the asymptotic behavior of (9) tends to a constant rate for a fixed number of users and a given set of channel gains. In contrast, our achievable secure sum rate in (8) scales logarithmic with P. To prove this, we only need to show that the first term in (8) grows with $\log(P)$ as the second term is constant with respect to

[1] Note that in Definition 1 we are interested in weak secrecy.

[2] The rates are determined by how closely the equations integer coefficients match the channel gains $\mathbf{h}_\ell$.

[3] The scaling factors can be absorbed into the the channel gains.

the power. Without loss of generality, let us assume $\mathrm{SNR}_\ell = \alpha_\ell P,\ \forall\ \ell$ and some $\alpha_\ell > 0$ (Note that according to the earlier discussion in Proposition 1, $\alpha_\ell > 1$ is allowed). Then we have,

$$\begin{aligned}
&\sum_{k=1}^{K} R_{comb,k} \\
&\overset{a}{\geq} \frac{K}{2}\log(P) + \frac{1}{2}\sum_{k=1}^{K}\log(\alpha_k) - \frac{1}{2}\log(K^K|\det(\mathbf{F})|^2) \\
&= \frac{K}{2}\log(P) + \frac{1}{2}\sum_{k=1}^{K}\log(\alpha_k) - \frac{K}{2}\left(\log(K) + \log(P)\right) \\
&+\frac{1}{2}\log(1+\|\mathbf{h}\|^2 P) - \frac{1}{2}\sum_{k=1}^{K}\log(\alpha_k) \\
&= \frac{1}{2}\log(1+\|\mathbf{h}\|^2 P) - \frac{K}{2}\log(K) \qquad (10)
\end{aligned}$$

where inequality (a) is deduced from Theorem 4 in [5]. Now, we exploit Theorem 12 in [5] in which it is shown that $R_{comb,k} < \frac{1+\delta(K-1)}{K+\delta(K-1)} \cdot \frac{1}{2}\log(P) + c,\ \forall\ k$, where the inequality holds for any $\delta > 0$ and some c constant with respect to P. Therefore, if we take $\delta \to 0$ and ignore the constant terms in (10), we have $\sum_{k=2}^{K} R_{comb,k} \propto \frac{1}{2} \cdot \frac{K-1}{K}\log(P)$. As a result, the secure sum rate in (8) grows with $\log(P)$.

The numerical results are given in Fig. 2 which are evaluated for the three-user channel and random i.i.d. (real) Gaussian channel gains. It can be seen that for the moderate and high SNR regimes, our proposed scheme outperforms the random coding result presented in [1]. Notice that the achievable non-secure results are shown in the figure as well which can be considered as an upper bound on the secure sum rate.

Another interesting observation occurs when the channel to the legitimate receiver is degraded with respect to the channel to the eavesdropper. For the Gaussian setting and the same noise power, this corresponds to the case $\|\mathbf{h}\| \leq \|\mathbf{g}\|$. In this case, according to the expression in (9), random coding fails to achieve a positive secure sum rate, while our scheme achieves a strictly positive secure sum rate as long as the ratios $\frac{\mathbf{h}_\ell}{\mathbf{g}_\ell}$ are not rational.[4] To illustrate this observation, we ran an experiment on a two-user Gaussian wiretap MAC with a fixed power (at SNR$= 25$dB) in which the channel gains are given as

$$\mathbf{h} = \left[1, \sqrt{2}\right]^T, \quad \mathbf{g} = \left[\sqrt{3}\cos(\theta), \sqrt{3}\sin(\theta)\right]^T \qquad (11)$$

for some random θ uniformly distributed over $[0, 2\pi]$. This is an example of the case where $\|\mathbf{h}\| = \|\mathbf{g}\|$. Fig. 3 shows that as long as the ratios of $\frac{h_\ell}{g_\ell}$ are not rational, a positive secure sum rate can be attained following our scheme.

At last, we investigate the asymptotic behavior of the expression (8). We show that our scheme achieves a total secure DoF of $\frac{K-1}{K}$. Earlier, to prove the scalability of (8) with $\log(P)$, we showed that the $R_{\textbf{sum}}$ is proportional to $\frac{1}{2} \cdot \frac{K-1}{K}\log(P)$, provided that the constant terms are ignored. Therefore,

$$\lim_{P\to\infty} \frac{R_{\textbf{sum}}}{\frac{1}{2}\log\left(1+P\right)} = \frac{K-1}{K} \qquad (12)$$

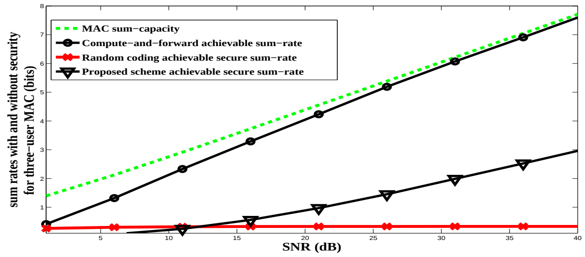

Fig. 2: Achievable sum rate, with and without security evaluated for the three-user asymmetric Gaussian MAC at different SNR.

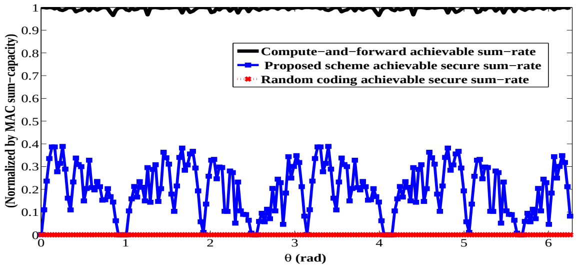

Fig. 3: Achievable sum rate evaluated for the two-user asymmetric Gaussian wiretap MAC with channel gains given as in (11) at SNR=25 dB.

Thus, the asymptotic behavior of the proposed scheme agrees with the result in [2]. In fact, we can further improve the presented scheme so that its asymptotic behavior reaches the optimal secure degrees of freedom given in [3]. The latter is aimed to be presented in the extended version.

IV. Proof of Theorem 1

In this section, we use notions and properties related to the lattice coding and nested lattice structure which are discussed in detail in the seminal work by Erez and Zamir in [7]. Due to the space limitation, we avoid discussing the previously known results in this paper and we focus on the new results. Our proposed scheme provides security by confusing the eavesdropper through aligning the codewords at the eavesdropper side such that it can only decode the subsets of the codewords which have the same sum values in $\mathbb{R}^N$. To this end, each encoded codeword $\tilde{\mathbf{x}}$ at transmitter ℓ is scaled before the transmission by a factor of $\frac{1}{g_\ell}$, i.e., $\mathbf{x}_\ell = \frac{\tilde{\mathbf{x}}_\ell}{g_\ell}$, so that the eavesdropper receives the sum of the codewords $\tilde{\mathbf{x}}$ as its channel output, i.e., $\mathbf{y}_E = \sum_{\ell=1}^{K}\tilde{\mathbf{x}} + \mathbf{z}_E$. Consequently, user ℓ generates its codewords $\tilde{\mathbf{x}}$ using power of $\mathrm{SNR}_\ell \triangleq g_\ell^2 P$ so that the transmitted codewords $\mathbf{x}_\ell$ satisfy the power constraint in (2).

As it was mentioned earlier, to address the problem of users with different powers, we utilize the asymmetric compute-and-forward framework along with a nested lattice structure. In our asymmetric compute-and-forward framework, user ℓ generates a sequence of n-length lattice codewords $\mathbf{t}_\ell$ using a pair of fine and coarse lattice sets as $(\Lambda_{f,\ell}, \Lambda_\ell)$. The coarse lattice Λ_ℓ is scaled such that its second moment equals to the available power at user ℓ, i.e., $\mathrm{SNR}_\ell = g_\ell^2 P$. Also, we impose a nested structure on the users' lattice pairs as

$$\Lambda_K \subseteq \Lambda_{K-1} \subseteq \cdots \subseteq \Lambda_1 \subseteq \Lambda_{f,K} \subseteq \cdots \subseteq \Lambda_{f,1} \qquad (13)$$

In the rest of the proof, we shall assume $\pi(\ell) = \ell,\ \forall\ \ell$ in (8). If that is not the case, we can simply re-index the users indices

[4] It can be shown that the Lebesgue measure of such rational ratios is small.

and define a nested structure as in (13) for the re-indexed users.

User ℓ constructs its codebook in three steps. The first step for user ℓ is to construct its inner codebook $\mathcal{L}_\ell \triangleq \Lambda_{f,\ell} \cap \mathcal{V}_\ell$, where $\mathcal{V}_\ell$ is the fundamental Voronoi region of the coarse lattice Λ_ℓ. The ratio between the coarse and the fine lattices is set such that $\mathcal{L}_\ell$ consists of $2^{nR_{comb,\ell}}$ inner codewords $\mathbf{t}_\ell$, i.e., $R_{comb,\ell} = \frac{1}{n}\log\left|\Lambda_{f,\ell} \cap \mathcal{V}_\ell\right|, \ \forall\ \ell$. The inner codewords $\mathbf{t}_\ell$ have a uniform distribution over $\mathcal{L}_\ell$.

In the second step, user ℓ builds its outer codebook by generating B i.i.d. copies of the inner codewords $\mathbf{t}_\ell$, for some large enough B. Let us denote the outer codewords as $\bar{\mathbf{t}}_\ell$. Then we have $\bar{\mathbf{t}}_\ell \triangleq [\mathbf{t}_\ell^{[1]}, \ldots, \mathbf{t}_\ell^{[B]}]$. Note that each $\mathbf{t}_\ell^{[i]}$ is independently and uniformly distributed over $\mathcal{L}_\ell$. It is worth to mention that the outer code is added only for technicality reasons in the proof of Lemma 2 in [8] and it does not increase secrecy. Also, adding the outer layer to the codebook changes the block length of the overall codewords from n to $N \triangleq B \times n$.

Finally, in the third step, the wiretap codebook is built. To this end, user ℓ partitions the outer codewords $\bar{\mathbf{t}}_\ell$ into 2^{NR_ℓ} equal-size bins and randomly assigns each index $w_\ell \in \{1, \ldots, 2^{NR_\ell}\}$ to exactly one bin. Rates R_ℓ are chosen such that they satisfy (6) and $\sum_{\ell=1}^{K} R_\ell = \sum_{\ell=2}^{K} R_{comb,\ell} - \frac{1}{2}\log\left(\frac{\sum_\ell g_\ell^2}{g_1^2}\right) + \epsilon_1$, for some small $\epsilon_1 > 0$. Also, user ℓ has a random dither $\mathbf{d}_\ell^{[i]}$ for each block i, which is independently generated according to a uniform distribution over $\mathcal{V}_\ell$. Dithers are public and do not increase secrecy.[5]

To send a message $W_\ell = w_\ell$, user ℓ randomly picks a codeword $\bar{\mathbf{t}}_\ell$ from the corresponding bin and dithers it. Then, it scales the resulting codeword by the factor of $\frac{1}{g_\ell}$. The signal transmitted by user ℓ is

$$\mathbf{x}_\ell \triangleq \frac{1}{g_\ell}\left(\left[\bar{\mathbf{t}}_\ell + \bar{\mathbf{d}}_\ell\right] \mod \Lambda_\ell\right) \qquad (14)$$

Note that in (14) the modular operation is done block-wise, meaning that for $i \in \{1, \ldots, B\}$ the signal transmitted at block i is $\frac{1}{g_\ell}([\mathbf{t}_\ell^{[i]} + \mathbf{d}_\ell^{[i]}] \mod \Lambda_\ell)$.

Proof of secrecy

In this subsection, we bound the eavesdropper's equivocation rate. Without loss of generality, let us assume $R_{comb,\ell} > 0, \ \forall\ \ell$. We have

$$\begin{aligned}
&\frac{1}{N}H(W_1, \ldots, W_K \big| \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K) \\
&\geq \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \big| \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K) \\
&- \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \big| W_1, \ldots, W_K, \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K) \\
&\overset{(a)}{\geq} \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \big| \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K) - 2\epsilon_2 \\
&\geq \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \big| \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K, \mathbf{z}_E) - 2\epsilon_2 \\
&\overset{(b)}{=} \frac{1}{N}H\left(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \middle| \sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K\right) - 2\epsilon_2
\end{aligned}$$

$$\begin{aligned}
&\overset{(c)}{=} \frac{1}{N}H\left(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \middle| \left[\sum_{\ell=1}^{K} \bar{\mathbf{t}}_\ell\right] \mod \Lambda_1, \bar{\mathbf{u}}_1, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K\right) - 2\epsilon_2 \\
&\overset{(d)}{=} \frac{1}{N}H\left(\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K \middle| \left[\sum_{\ell=1}^{K} \bar{\mathbf{t}}_\ell\right] \mod \Lambda_1, \bar{\mathbf{u}}_1, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K\right) - 2\epsilon_2 \\
&\overset{(e)}{\geq} \frac{1}{N}H\left(\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K \middle| \left[\sum_{\ell=1}^{K} \bar{\mathbf{t}}_\ell\right] \mod \Lambda_1\right) - \frac{1}{N}H(\bar{\mathbf{u}}_1) - 2\epsilon_2 \\
&\overset{(f)}{=} \frac{1}{N}H(\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K) - \frac{1}{N}H(\bar{\mathbf{u}}_1) - 2\epsilon_2 \\
&\overset{(g)}{=} \frac{B}{N}\sum_{\ell=2}^{K} nR_{comb,\ell} - \frac{B}{N}H(\mathbf{u}_1^{[1]}) - 2\epsilon_2 \\
&\overset{(h)}{\geq} \sum_{\ell=2}^{K} R_{comb,\ell} - (1-\epsilon)\frac{1}{2}\log\left(\frac{\sum_{\ell=1}^{K} g_\ell^2 + \epsilon}{g_1^2}\right) - \delta(\epsilon) - 2\epsilon_2 \\
&\geq \sum_{\ell=2}^{K} R_{comb,\ell} - \frac{1}{2}\log\left(\frac{\sum_{\ell=1}^{K} g_\ell^2}{g_1^2}\right) - \frac{\epsilon}{g_1^2} - \delta(\epsilon) - 2\epsilon_2 \\
&\overset{(i)}{=} \sum_{\ell=2}^{K} R_{comb,\ell} - \frac{1}{2}\log\left(\frac{\sum_{\ell=1}^{K} g_\ell^2}{g_1^2}\right) - \epsilon_3 \qquad (15)
\end{aligned}$$

In the above inequalities, (a) is deduced from applying the packing lemma to the outer codewords (detailed proof of this step is provided in Appendix of [8]). (b) is true since after subtracting the noise from $\mathbf{y}_E$, the remaining random vectors become independent of the noise. (c) is true since Λ_1 is the densest lattice among the lattices $(\Lambda_1, \Lambda_2, \ldots, \Lambda_K)$, according to the nested structure in (13). Therefore,

$$\left[\sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell - \sum_{\ell=1}^{K} \bar{\mathbf{d}}_\ell\right] \mod \Lambda_1 = \left[\sum_{\ell=1}^{K} \bar{\mathbf{t}}_\ell\right] \mod \Lambda_1.$$

Also, notice that

$$H\left(\sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell\right) = H\left(\left[\sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell\right] \mod \Lambda_1, \bar{\mathbf{u}}_1\right),$$

where $\bar{\mathbf{u}}_1 \triangleq \sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell - \left[\sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell\right] \mod \Lambda_1$. Inequality (d) is due to the reason that the codeword $\bar{\mathbf{t}}_1$ can be obtained from the modulo-sum $\left[\sum_{\ell=1}^{K} \bar{\mathbf{t}}_\ell\right] \mod \Lambda_1$ and the sequence of codewords $\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K$. (e) holds since dithers are independent of the codewords and conditioning reduces entropy. (f) is deduced from Lemma 2 in [9] (Crypto lemma), which implies that for each block $i \in [1, B]$, $\left[\mathbf{t}_1^{[i]} + \sum_{\ell=2}^{K} \mathbf{t}_\ell^{[i]}\right] \mod \Lambda_1$ has uniform distribution over the codebook $\mathcal{L}_1$ and is independent of $\sum_{\ell=2}^{K} \mathbf{t}_\ell^{[i]}$. (g) is true since $\left|\mathcal{L}_\ell\right| = 2^{nR_{comb,\ell}}$ and for $i \in \{1, \ldots, B\}$, inner codewords $\mathbf{t}_\ell^{[i]}$ have i.i.d. uniform distribution over $\mathcal{L}_\ell, \ \forall\ \ell$. Also, $\bar{\mathbf{u}}_1$ consists of B i.i.d. copies of $\mathbf{u}_1^{[i]}$ by its definition. (h) follows from applying Lemma 1 in Appendix to $\mathbf{u}_1^{[1]}$, and finally, (i) is deduced by defining $\epsilon_3 \triangleq \delta(\epsilon) + \frac{\epsilon}{g_1^2} + 2\epsilon_2$. Thus, the condition in (4) is satisfied and the proof of secrecy is completed.

V. Conclusion

In this paper, we proposed a security scheme built on the asymmetric compute-and-forward framework, which works at

[5] As the average leakage rate (w.r.t. dithers) goes to zero, there must exist a sequence of deterministic dithers for which the leakage rate goes to zero.

any finite SNR. The achievable secure sum rate presented in our scheme scales with $\log(\mathrm{SNR})$ and therefore, it significantly outperforms the existing random coding result for the most SNR regimes. Our presented scheme also achieves a total secure DoF of $\frac{K-1}{K}$. This result can be furthered improved to achieve the optimal secure DoF which is aimed to be presented in our future work.

Acknowledgment

The authors would like to thank Bobak Nazer and Prakash Ishwar for their valuable comments and helpful discussions.

References

[1] E. Tekin and A. Yener, “The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[2] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, “On the secure degrees-of-freedom of the multiple-access-channel,” available online http://arxiv.org/abs/1003.0729.

[3] J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” Submitted September 2012, available online http://arxiv.org/abs/1209.5370.

[4] B. Nazer and M. Gastpar, “Compute-and-forward: Harnessing interference through structured codes,” *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.

[5] O. Ordentlich, U. Erez, and B. Nazer, “The approximate sum capacity of the symmetric gaussian k-user interference channel,” *IEEE Transactions on Information Theory*, To appear 2014, available online http://arxiv.org/abs/1206.0197.

[6] V. Ntranos, V. R. Cadambe, B. Nazer, and G. Caire, “Asymmetric compute-and-forward,” in *51th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, September 2013.

[7] U. Erez and R. Zamir, “Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding,” *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.

[8] P. Babaheidarian and S. Salimi, “Compute-and-forward can buy sececy cheap (extended version),” *preprint available at http://blogs.bu.edu/parisabh/files/2015/01/Extendedversion.pdf*, 2015.

[9] G. D. Forney, “On the role of mmse estimation in approaching the information-theoretic limits of linear gaussian channels: Shannon meets wiener,” in *41th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, September 2003.

Appendix

Lemma 1: Consider a set of n-dimensional lattices $\Lambda_1,\ldots,\Lambda_K$ with their fundamental Voronoi regions as $\mathcal{V}_1,\ldots,\mathcal{V}_K$, respectively. Assume that all the lattices are scaled such that their second moments equal to $\mathrm{SNR}_\ell = g_\ell^2 P,\ \forall\, \ell \in \{1,\ldots,K\}$, where $P>0$. Now construct random vectors $\mathbf{u}_j$, for $j \in \{1,\ldots,K\}$, as $\mathbf{u}_j \triangleq Q_{\Lambda_j}\left(\sum_{\ell=1}^K \mathbf{s}_\ell\right)$, where $\mathbf{s}_1,\ldots,\mathbf{s}_K$ are independent n-dimensional random vectors uniformly distributed over $\mathcal{V}_1,\ldots,\mathcal{V}_K$, respectively, and the operation $Q_{\Lambda_j}(.)$ is the nearest neighbor quantizer with respect to the lattice Λ_j. Then, for all $\epsilon>0$ and sufficiently large n, the entropy of $\mathbf{u}_j$ is bounded as

$$\frac{1}{n}H(\mathbf{u}_j) \leq (1-\epsilon)\frac{1}{2}\log\left(\frac{\sum_{\ell=1}^K g_\ell^2+\epsilon}{g_j^2}\right)+\delta(\epsilon) \quad \forall j \tag{16}$$

where $\delta(\epsilon)$ tends to zero as $\epsilon \to 0$.

Proof: According to Lemma 1, $\mathbf{u}_j$ is the output of the lattice quantizer Q_{Λ_j}, so it can only take discrete values. To bound the entropy of $\mathbf{u}_j$, first we bound the range of $\|\sum_{\ell=1}^K \mathbf{s}_\ell\|$ as follows. Let $r_{\mathrm{cov},\ell}$ denote the covering radius of Λ_ℓ, i.e., the radius of the smallest ball containing the Voronoi region $\mathcal{V}_\ell$. Also, let $r_{\mathrm{eff},\ell}$ denote the radius of the sphere which has the same volume as the volume of $\mathcal{V}_\ell$, i.e., $\mathrm{Vol}(B(r_{\mathrm{eff},\ell})) = \mathrm{Vol}(\mathcal{V}_\ell)$. Now, consider K (n-dimensional) balls whose second moments per dimension equal to $\sigma_1^2,\sigma_2^2,\ldots,\sigma_K^2$ and their radii are given as $r_{\mathrm{cov},1}, r_{\mathrm{cov},2},\ldots,r_{\mathrm{cov},K}$, respectively. Next, for each $\ell \in \{1,\ldots,K\}$, consider a random vector $\mathbf{b}_\ell$ with the uniform distribution over an n-dimensional ball $B(r_{\mathrm{cov},\ell})$. Recall that a ball has the smallest normalized second moment for a given volume [7]. Therefore, we have

$$\begin{aligned} g_\ell^2 P &= \frac{1}{n}\mathbb{E}\|\mathbf{s}_\ell\|^2 \\ &\geq \frac{1}{n}\mathbb{E}\left\|\left(\frac{r_{\mathrm{eff},\ell}}{r_{\mathrm{cov},\ell}}\right)\mathbf{b}_\ell\right\|^2 = \left(\frac{r_{\mathrm{eff},\ell}}{r_{\mathrm{cov},\ell}}\right)^2\sigma_\ell^2,\ \forall\ \ell \end{aligned} \tag{17}$$

Now, consider a random vector $\mathbf{z}_{eq} \triangleq \sum_{\ell=1}^K \mathbf{z}_\ell$, in which random vectors $\mathbf{z}_\ell$ are i.i.d. according to the distribution $\mathcal{N}(\mathbf{0},\sigma_\ell^2\mathbf{I})$ and therefore, $\mathbf{z}_{eq} \sim \mathcal{N}(\mathbf{0},\sigma_{eq}^2\mathbf{I})$. Then, from (17) we have $\sigma^2_{\mathbf{z}_{eq}} = \sum_{\ell=1}^K \sigma_\ell^2 \leq \sum_{\ell=1}^K \left(\frac{r_{\mathrm{cov},\ell}}{r_{\mathrm{eff},\ell}}\right)^2 g_\ell^2 P$. Now, using Lemma 11 in [7], we conclude that

$$\begin{aligned} &e^{K.n.c(n)} f_{\mathbf{z}_{eq}}(\mathbf{z}_{eq}) = e^{K.n.c(n)}\left(f_{\mathbf{z}_1}(\mathbf{z}_{eq}) * \ldots * f_{\mathbf{z}_K}(\mathbf{z}_{eq})\right) \\ &\geq f_{\sum_{\ell=1}^K \mathbf{s}_\ell}(\mathbf{z}_{eq}) \end{aligned} \tag{18}$$

where $n.c(n)$ goes to zero as n goes to infinity. Notice that in deriving (18) we also used the fact that vectors $\mathbf{s}_\ell$ are independent vectors, and hence, pdf of their sum is the convolution of their individual pdfs. Now we can bound the range of $\|\sum_{\ell=1}^K \mathbf{s}_\ell\|$ as follows. For any $\epsilon>0$,

$$\begin{aligned} &\Pr\left(\|\sum_{\ell=1}^K \mathbf{s}_\ell\| \notin B\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right) \\ &\overset{(a)}{\leq} e^{K.n.c(n)}\Pr\left(\|\mathbf{z}_{eq}\| \notin B\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right) \leq \epsilon. \end{aligned}$$

Inequality (a) follows from (18) and non-negativity of the ℓ_2-norm. Also, the last inequality is deduced from the Weak Law of Large numbers (WLL) for sufficiently large n. Since we showed that $\|\sum_{\ell=1}^K \mathbf{s}_\ell\|$ belongs to the ball $B(\sqrt{n\sigma^2_{zeq}+n\epsilon})$ with probability $1-\epsilon$, it only remains to find an upper bound on the number of non-intersecting Voronoi regions $\mathcal{V}_j$ which fit in this ball, i.e.,

$$\begin{aligned} &\frac{Vol\left(\mathcal{B}\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right)}{Vol\left(\mathcal{V}_j\right)} = \frac{Vol\left(\mathcal{B}\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right)}{Vol\left(B(r_{\mathrm{eff},j})\right)} \\ &\overset{(a)}{\leq} \left(\frac{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}{\left(\frac{r_{\mathrm{eff},j}}{r_{\mathrm{cov},j}}\right)^2 n g_j^2 P}\right)^{\frac{n}{2}} \overset{(b)}{\leq} \left(\frac{\sum_{\ell=1}^K \left(\frac{r_{\mathrm{cov},\ell}}{r_{\mathrm{eff},\ell}}\right)^2 g_\ell^2+\epsilon}{\left(\frac{r_{\mathrm{eff},j}}{r_{\mathrm{cov},j}}\right)^2 g_j^2}\right)^{\frac{n}{2}}, \end{aligned}$$

where inequality (a) is concluded from Lemma 6 in [7] and inequality (b) follows from (17). Finally, recall that for a high dimensional good lattices, we have $\log\left(\frac{r_{\mathrm{cov},\ell}}{r_{\mathrm{eff},\ell}}\right) \to 0$ [7]. Therefore,

$$\frac{1}{n}H(\mathbf{u}_j) \leq (1-\epsilon)\frac{1}{2}\log\left(\frac{\sum_{\ell=1}^K g_\ell^2+\epsilon}{g_j^2}\right)+\delta(\epsilon).$$

Note that using WLL, the term $\delta(\epsilon)$ tends zero as n goes to infinity. This completes the proof. ■